UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,574	12/09/2004	Brian Albert Wittman	PU020277	1365

7590 11/21/2008

Joseph S Tripoli
Thomson Licensing Inc
PO Box 5312
Princeton, NJ 08543-5312

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
11/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/517,574	**Applicant(s)** WITTMAN, BRIAN ALBERT	
	Examiner MICHAEL R. VAUGHAN	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 November 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-19* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/517574 filed on 12/9/04 and amended on 11/05/08 is presented for examination by the examiner. Examiner has carefully considered Applicant's remarks and arguments. Applicant has amended claims 1, 4, 7, 10, 13, and 16-19 and canceled claim 2. Claims 1 and 3-19 are pending.

Response to Amendment

Having considered the presented amendments, Examiner hereby withdraws the previous rejections under 35 USC 101 for claims 1-15.

Response to Arguments

Applicant's arguments with respect to claims 1 and 2-19 have been considered but are moot in view of the new ground(s) of rejection. In response to the newly amended claims, Examiner finds teaching of those new limitations in prior art ZoneAlarm 2.6 released to the public on August 1, 2001. Examiner is relying on a publication from PC Update, authored by Ash Nallawalla from May 2002 which expounds upon some of the features of ZoneAlarm 2.6 from that time. Examiner is also supplying two other publications giving some details of ZoneAlarm's functionality. In addition to those publications, Examiner is also listing the original patents for ZoneAlarm for Applicant's considerations as well. Please see Examiner's arguments with regard to ZoneAlarm and its application to the claim language below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-4, and 6-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Application Publication 2002/0133586 A1 to Shanklin et al hereinafter Shanklin in view of ZoneAlarm publication by Ash Nallawalla hereinafter ZoneAlarm.

As per claim 1, Shanklin teaches an apparatus adapted to communicate via a network, comprising a firewall [0013], including a set of rules [set of parameters] for identifying packets associated with inappropriate activity (0074). Shanklin teaches having an indicator for when the rule are broken by inappropriate packet (0073). Shanklin is silent is expressly teaching separating those sets of rules into a plurality of classes and an indicator device for providing a plurality of user discernable indicators, wherein each of the plurality of user discernable indicators is associated with a different one of the plurality of classes, and wherein a respective one of said plurality of user discernable indicators is triggered if one or more of said plurality of rules corresponding to one of said plurality of classes associated with the respective one of said plurality of user discernable indicators is violated. ZoneAlarm teaches sets of rules into a plurality of classes and an indicator device for providing a plurality of user discernable indicators, wherein each of the plurality of user discernable indicators is associated with a different one of the plurality of classes, and wherein a respective one of said plurality of user discernable indicators is triggered if one or more of said plurality of rules corresponding to one of said plurality of classes associated with the respective one of said plurality of user discernable indicators is violated (pgs 2 and 4). ZoneAlarm is able to govern different sets of classes. Those classes are outgoing traffic, incoming traffic, identifying/privacy data, and malicious code. Examiner interprets these different categories of protection as classes. ZoneAlarm protects the user from each of these types of classes, each posing their own unique type of threat to a user and his/her network. What is unique about ZoneAlarm is that each type of classes has its own set of rules governing those specific classes. Certain classes can have higher levels of protection and can even break down those classes into zones whereby different rules can be applied to the different zones. For example, one could block all inbound traffic from an internet zone, and allow all inbound traffic from a trusted zone. ZoneAlarm also provides different visual indicators for when rules are broken for each type of class. The indicators themselves are unique to each class and are color coded. For example in Figure 3, on page 2, an inbound threat trigger is shown displayed in red. On page 4, in figure 7, an outbound threat trigger is displayed in Orange. Another unique visual indicator is shown on page 4, in figure 8 as a response to a privacy threat trigger. Creating classes of threats and having specific triggers for those threats give the user a more control and easier manageability of his/her system. Combining prior art elements according to known methods to yield predictable results is obvious. All the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination would have yielded predictable results to one or ordinary skill in the art at the time of the invention.

As per claim 3, Shanklin teaches an apparatus
comprises at least one of a modem, a router, and a bridge [0080].

As per claim 4, Shanklin teaches and indicator comprises
at least one visual indicator (alert to admin) [0105].

As per claim 5, Shanklin teaches alerting the administrator but is silent is expressly disclosing one type of visual indicator comprises a light emitting device proximate to the apparatus. ZoneAlarm teaches one type of visual indicator comprises a light emitting device proximate to the apparatus (pg. 2, figure 3). The visual indicator is displayed on a PC monitor which is a light emitting device. Examiner relies upon same rationale for combining Shanklin and ZoneAlarm as recited above.

As per claim 6, Shanklin teaches one visual indicator comprises a highlighted icon (alert to admin) displayed on a computing device [0105].

As per claim 7, Shanklin teaches defining a set of rules to detect inappropriate communication activity on a computer or network (0074); examining data traffic to determine whether at least one of the rules has been violated (0074). Shanklin is silent is explicitly teaching separating the rules in the set into a plurality of classes;

associating each of the plurality of classes with a different one of a plurality of user discernable indicators; and in the case that at least one of the rules of a first one of said plurality of classes has been violated, filtering said data traffic violating the at least one of the rules of the first one of said plurality of classes and providing a user discernable notification of said violation by triggering a respective one of the plurality of user discernable indicators associated with the first one of said plurality of classes. ZoneAlarm teaches separating the rules in the set into a plurality of classes; associating each of the plurality of classes with a different one of a plurality of user discernable indicators; and in the case that at least one of the rules of a first one of said plurality of classes has been violated, filtering said data traffic violating the at least one of the rules of the first one of said plurality of classes and providing a user discernable notification of said violation by triggering a respective one of the plurality of user discernable indicators associated with the first one of said plurality of classes. Examiner relies upon the same rational for combining Shanklin and ZoneAlarm as recited in the rejection of claim 1.

As per claim 8, Shanklin teaches determining if a first threshold level of rule violation has been exceeded prior to filtering said data traffic [0074]. In one embodiment Shanklin teaches monitoring traffic and then if the numbers of packets exceed a safe level during a time, denying access to said packets.

As per claim 9, Shanklin teaches determining if a first threshold level of rule [0076] violation has been exceeded prior to triggering the user discernable indicator (alert) [0074].

As per claim 10, Shanklin teaches in the case of at least one of the rules of a second one of said plurality of classes being violated, filtering said data traffic violating the at least one of the rules of the second one of said plurality of classes and triggering a particular one of said plurality of user discernable indicators associated with the second one of the plurality of classes (0074-0079). Shanklin explicitly teaches different classes of threats and how to handle those threats based on rules set by an admin. Shanklin teaches there can be any number of these rule classes (including a second or third) and that different responses and even combinations of responses applicable based on the level of the threat.

As per claim 11, Shanklin teaches determining if a second threshold level of rule violation has been exceeded prior to filtering said data traffic [0076].

As per claim 12, Shanklin teaches determining if a second threshold level of rule violation has been exceeded prior to triggering the user discernable indicator [0074-0076].

As per claim 13, Shanklin teaches a case of a rule of a third class being violated, filtering said data traffic violating said third class rule; and triggering the user discernable indicator [0074-0079]. Shanklin explicitly teaches different classes of threats and how to handle those threats based on rules set by an admin. Shanklin teaches there can be any number of these rule classes (including a second or third) and that different responses and even combinations of responses applicable based on the level of the threat. ZoneAlarm also teaches at least up to 4 classes.

As per claim 14, Shanklin teaches determining if a third threshold level of rule violation has been exceeded prior to filtering said data traffic [0068 and 0035].

As per claim 15, Shanklin teaches determining if a third threshold level of rule violation has been exceeded prior to triggering the user discernable indicator [0073].

Claims 16 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin in view of ZoneAlarm and in view of USP 6,185,624B1 to Fijolek et al, hereinafter Fijolek.

As per claim 16, Shanklin teaches a firewall program having associated with it a set of rules [0074], said firewall program including a set of rules for identifying packets associated with inappropriate activity (0074), resident in said memory and executable by said controller (mid-network switching device i.e. Switch) to cause examining data (monitoring) of packets from said downstream (internal network) and upstream circuitry (internet) [0034]. While Shanklin teaches that his invention is carried out in a mid-network switch device, he does not explicitly teach of a cable modem being used. He does give an example of a router which one of skill in the art would know performs certain basic hardware functions. One of skill in the art would also know a mid-network switching device has internal circuitry including a controller and memory. Fijolek teach the use of a cable modem which has all of these features (upstream, downstream, controller, memory, and able to communicate data packets across a network (col. 2, lines 5-10 and col. 8, 45-55). Moreover, Fijolek teaches that his cable modem has management software whereby an admin can program it via a network. This is precisely the feature taught by Shanklin's invention. One skilled in the art could see that the cable modem of Fijolek can perform the methods of Shanklin's invention. One of ordinary skill in the art would have reasonable expectations of success and be motivated to protect the network from end to end. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shanklin with the teaching of Fijolek; namely to use a cable modem as a mid-network switching device. Shanklin is silent is expressly teaching separating those sets of rules into a plurality of classes and an indicator device for providing a plurality of user discernable indicators, wherein each of the plurality of user discernable indicators is associated with a different one of the plurality of classes, and wherein a respective one of said plurality of user discernable indicators is triggered if one or more of said plurality of rules corresponding to one of said plurality of classes associated with the respective one of said plurality of user discernable indicators is violated. ZoneAlarm teaches sets of rules into a plurality of classes and an indicator device for providing a plurality of user discernable indicators, wherein each of the plurality of user discernable indicators is associated with a different one of the plurality of classes, and wherein a respective one of said plurality of user discernable indicators is triggered if one or more of said plurality of rules corresponding to one of said plurality of classes associated with the respective one of said plurality of user discernable indicators is violated (pgs 2 and

4). Examiner relies upon the same rationale for combining Shanklin and ZoneAlarm as recited in the rejection of claim 1.

As per claim 19, Shanklin teaches one visual indicator comprises a highlighted icon (alert message sent to admin) displayed on a computer device (0073).

Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin, ZoneAlarm, and Fijolek as applied to claim 16 above, and further in view of USP Application Publication 2002/0080784 to Krumel.

As per claim 17, Shanklin combined with ZoneAlarm teaches a plurality of user discernable indicators including alerts being sent to a system administrator in the event of a security event of some kind. Shanklin, ZoneAlarm, and Fijolek are silent in explicitly disclosing that one type of alert could be a light emitting diode. Krumel teaches the use of light emitting diodes aka LEDs to provide visual feedback of the data protection system status [0108]. Krumel also explicitly teaches that LEDs are preferable in providing alarm type information. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Shanklin with the teaching of Krumel by incorporating the LEDs of Krumel as a means to alert the administrator of a security system in Shanklin.

As per claim 18, Shanklin combined with ZoneAlarm teaches a plurality of user discernable indicators of alerting an admin when certain security rules and thresholds are exceeded [0074-0079]. Shanklin mentioned that the system monitors events and notifies the admin via a number of ways based on the security event. Shanklin, ZoneAlarm, and Fijolek are silent in disclosing that the plurality of user discernable indicator comprises a first LED for signifying a filtering event and a second LED for signifying filtering data packets deemed pernicious in a set of rules. Krumel teaches the use of LEDs to provide visual feedback of the data protection system status. More specifically Krumel teaches a multiple LEDs [0109] to provide feedback based on the event [0108]. As an example Krumel teaches using a first LED to indicate the protection system is filtering one or more packets. Krumel then teaches using a second LED to indicate the system is under attack [0108]. It would have been obvious to one of ordinary skill in the art the time of the invention to modify the combined teachings of Shanklin, ZoneAlarm, and Fijolek with the teachings of Krumel. The use of LEDs as taught by Krumel would improve the feedback in the combined system of Shanklin and Fijolek. It would provide quick visual stimuli to alert the admin on what is occurring in their network. One of ordinary skill in the art would be motivated to respond to a threat as quick as possible. Knowing how severe the threat is based on the visual indicia prevents the case of over reacting to every single security event.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is listed on the enclosed PTO-892 form.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MRV
2431
/Syed Zia/
Primary Examiner, Art Unit 2431